

# Starting up a Cypress AMI

The Cypress Certification tool provides an Amazon Machine Image (AMI) that should allow you to easily start up an instance of the Cypress application. An AMI is a virtual machine template that can be used to clone an instance of an Amazon Elastic Compute Cloud virtual machine. Amazon Virtual machines can be run for a low cost hourly fee (see: <http://aws.amazon.com/ec2/pricing/>). The following instructions will walk you through cloning your own instance and finalizing the instance of Cypress.

## EC2 Dashboard

Begin by going to the Amazon EC2 console:

<https://console.aws.amazon.com/console/home>

Log into the EC2 console using an amazon account, or create a new account. On the Main screen select the EC2 link under Amazon Web Services.



The screenshot shows the Amazon Web Services console home page. A green arrow points to the EC2 link under the Compute & Networking section. The text "Click the EC2 Link" is overlaid on the arrow. The console displays various AWS services categorized into Compute & Networking, Database, Analytics, Storage & Content Delivery, Deployment & Management, App Services, and Additional Resources. The EC2 link is highlighted with a green arrow and the text "Click the EC2 Link".

**Amazon Web Services**

- Compute & Networking**
  - Direct Connect: Dedicated Network Connection to AWS
  - EC2: Virtual Servers in the Cloud
  - Route 53: Scalable Domain Name System
  - VPC: Isolated Cloud Resources
- Database**
  - DynamoDB: Predictable and Scalable NoSQL Data Store
  - ElastiCache: In-Memory Cache
  - RDS: Managed Relational Database Service
  - Redshift: Managed Petabyte-Scale Data Warehouse Service
- Analytics**
  - Data Pipeline: Orchestration for Data-Driven Workflows
  - Elastic MapReduce: Managed Hadoop Framework
  - Kinesis: Real-time Processing of Streaming Big Data
- Storage & Content Delivery**
  - CloudFront: Global Content Delivery Network
  - Glacier: Archive Storage in the Cloud
  - S3: Scalable Storage in the Cloud
  - Storage Gateway: Integrates On-Premises IT Environments with Cloud Storage
- Deployment & Management**
  - CloudFormation: Templated AWS Resource Creation
  - CloudTrail: User Activity and Change Tracking
  - CloudWatch: Resource and Application Monitoring
  - Elastic Beanstalk: AWS Application Container
  - IAM: Secure AWS Access Control
  - OpsWorks: DevOps Application Management Service
- App Services**
  - CloudSearch: Managed Search Service
  - Elastic Transcoder: Easy-to-use Scalable Media Transcoding
  - SES: Email Sending Service
  - SNS: Push Notification Service
  - SQS: Message Queue Service
  - SWF: Workflow Service for Coordinating Application Components

**Additional Resources**

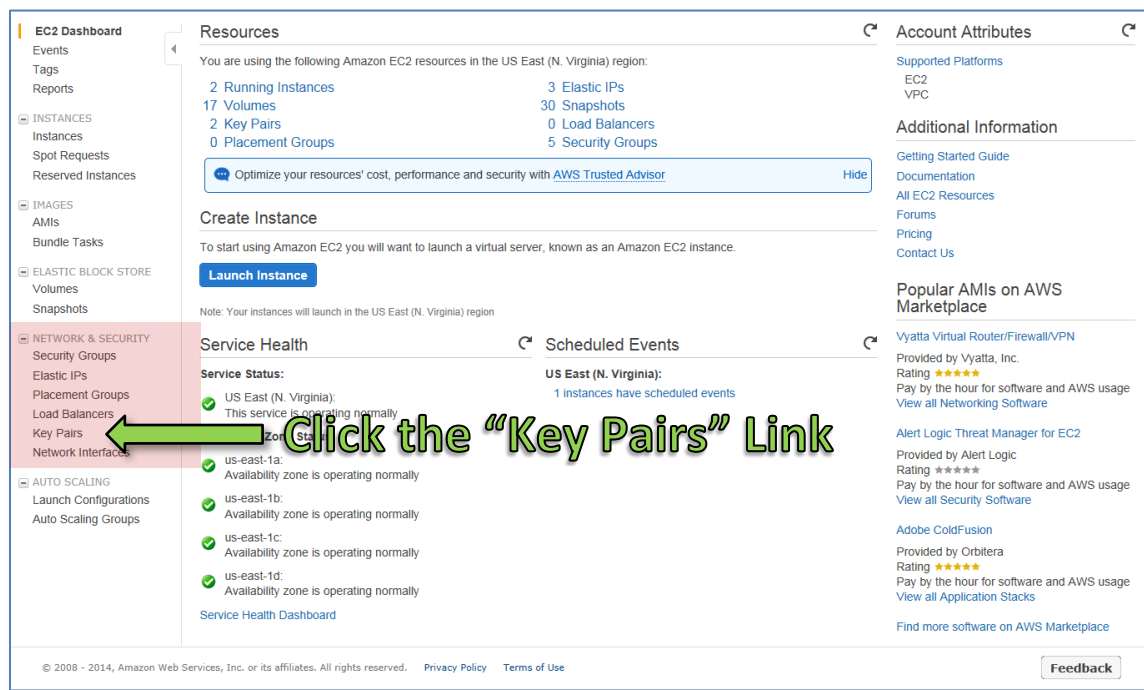
- Getting Started**  
See our documentation to get started and learn more about how to use our services.
- Trusted Advisor**  
Best practice recommendations to save money, improve fault tolerance, increase performance, and close security gaps.
- Service Health**  
All services operating normally.  
Updated: Feb 12 2014 11:33:00 EST  
[Service Health Dashboard](#)
- Set Start Page**  
Console Home
- AWS Marketplace**  
Find & buy software, launch with 1-Click and pay by the hour.

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Feedback](#)

The EC2 Dashboard screen should then appear. It provides the necessary functions for creating and managing your instance. If you do not already have a Key Pair, it will be necessary for you to create one. If you do have a Key Pair, skip ahead to the section “Create and Launch Instance”.

## Create Key Pair

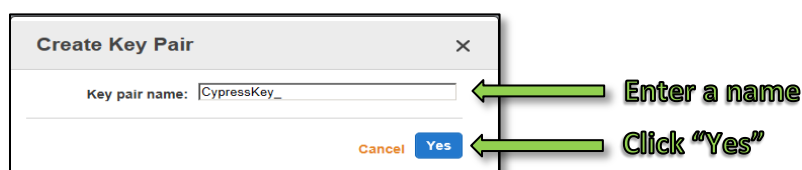
Click the “Key Pairs” link under the “Network & Security” section on the left side of the screen.



The “Key Pairs” screen that appears is used to create a key pair consisting of public and private keys used for secure access to the service. Click the “Create Key Pair” button.

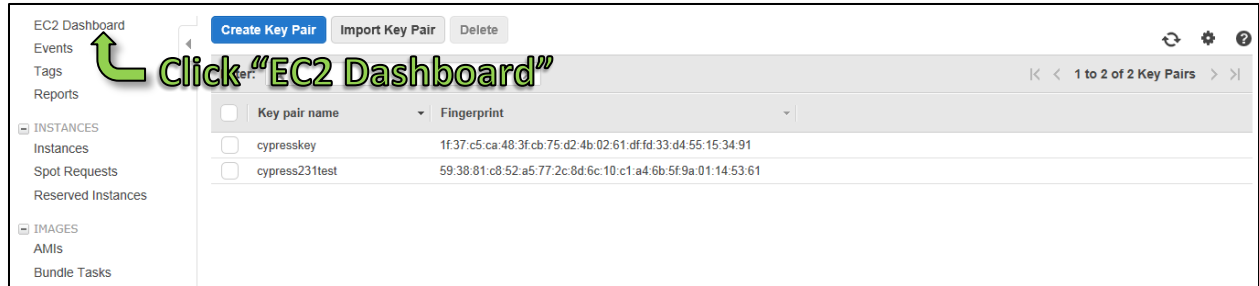


Enter a name for the key pair in the resulting window and click the “Yes” button.



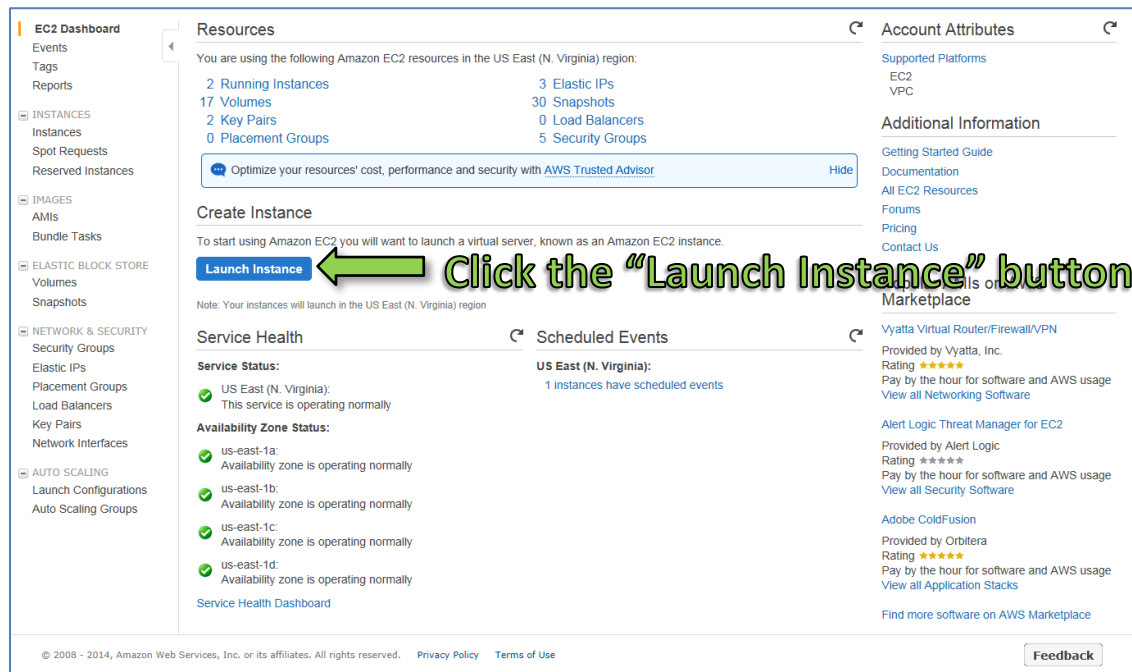
You will then be prompted by your browser to save the key file generated by Amazon. Save this file to a location you will easily remember as you will need it later.

Return to the EC2 dashboard screen by clicking “EC2 Dashboard” on the left side of the screen.

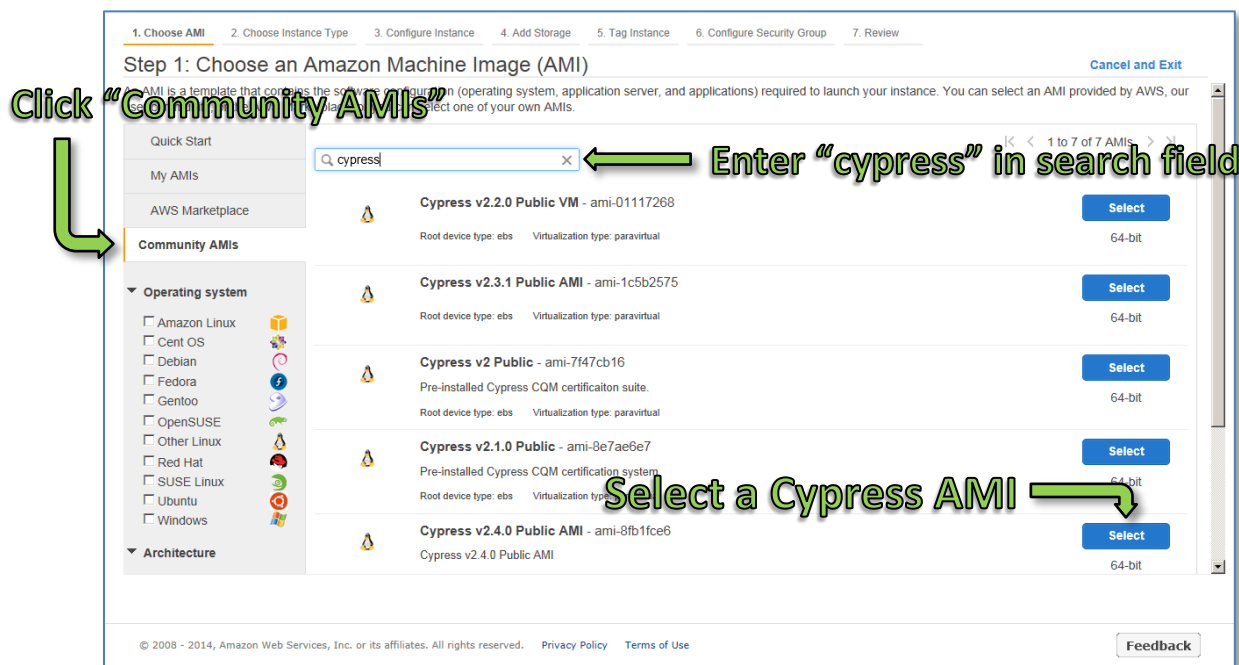


## Create and Launch Instance

Click the “Launch Instance” button on the EC2 dashboard screen.



In the resulting “Choose an Amazon Machine Image” screen, click the “Community AMIs” category on the left side of the screen, and enter “cypress” in the search field to find the available Cypress images. Click the ‘Select’ button next to the Cypress AMI you wish to use.



The “Choose an Instance Type” screen should then appear. Select the “All Instance Types” category on the left side of the screen, and select the “m1.medium” instance type in the table. Click the “Next: Configure Instance Details” button.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Currently selected: m1.medium (2 ECUs, 1 vCPUs, 3.7 GiB memory, 1 x 410 GiB Storage Capacity)

**All instance types** ← Click “All Instance Types”

Select an instance type to suit your requirements

Size	ECUs	vCPUs	Memory	Instance Storage	EBS-Optimized	Network Performance
t1.micro	up to 2	1	0.613	EBS only	-	Very Low
m1.small	1	1	1.7	1 x 160	-	Low
<b>m1.medium</b>	<b>2</b>	<b>1</b>	<b>3.7</b>	<b>1 x 410</b>	<b>-</b>	<b>Moderate</b>
m1.large	4	2	7.5	2 x 420	Yes	Moderate
m1.xlarge	8	4	15	4 x 420	Yes	Moderate
m3.medium	3	1	3.75	1 x 4 (SSD)	-	Moderate

Click “Next: Configure Instance Details”

Cancel Previous **Review and Launch** Next: Configure Instance Details

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Feedback](#)

The “Configuration Instance Details” screen should appear. Verify that the default settings match the following illustration, and click the “Next: Add Storage” button.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

**Number of instances** 1

**Purchasing option** ☐ Request Spot Instances

**Network** Launch into EC2-Classical [Create new VPC](#)

**Availability Zone** No preference

**IAM role** None

**Shutdown behavior** Stop

**Enable termination protection** ☐ Protect against accidental termination

**Monitoring** ☐ Enable CloudWatch detailed monitoring [Additional charges apply.](#)

Advanced Details

Cancel Previous **Review and Launch** Next: Add Storage

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Feedback](#)

In the “Add Storage” screen, set the machine size to 20 GB, and click “Next: Tag Instance”.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

### Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GB)	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-b7565ebb	20	Standard	N/A	<input checked="" type="checkbox"/>
Instance Store 0	/dev/sdb	N/A	N/A	N/A	N/A	N/A

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Tag Instance](#)

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Feedback](#)

In the “Tag Instance” screen, enter a name for your Cypress instance in the “Value” field, and click “Next: Configure Security Group”.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

### Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

**Key** (127 characters maximum) **Value** (255 characters maximum)

Name Cypress v2.4.0 AMI

[Create Tag](#) (Up to 10 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Feedback](#)

The “Configure Security Group” screen should then appear.

On the “Configure Security Group” screen, enter a security group name and description in the fields provided. There should already be a security rule in place for the SSH protocol. Add another rule for the HTTP protocol. Click the “Add Rule” button and select “HTTP” in the protocol drop-down list. The default settings for “Type”, “Port Range”, and “Source” should be as shown below.

The screenshot shows the 'Step 6: Configure Security Group' page in the AWS Management Console. The page has a breadcrumb trail at the top: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance, 6. Configure Security Group (active), 7. Review. Below the breadcrumb, there's a title 'Step 6: Configure Security Group' and a descriptive paragraph. The main section is 'Assign a security group:', with two radio buttons: 'Create a new security group' (selected) and 'Select an existing security group'. Below this are two text input fields: 'Security group name:' with the value 'Cypress\_Group' and 'Description:' with the value 'Cypress Security Group'. To the right of these fields is a green arrow pointing to them with the text 'Enter a group name and description'. Below the inputs is a table with four columns: 'Protocol', 'Type', 'Port Range (Code)', and 'Source'. The first row is for 'SSH' (Protocol), 'TCP' (Type), '22' (Port Range), and 'Anywhere' (Source). The second row is for 'HTTP' (Protocol), 'TCP' (Type), '80' (Port Range), and 'Anywhere' (Source). A green arrow points to the 'HTTP' dropdown in the first row with the text 'Click "Add Rule"'. Another green arrow points to the 'HTTP' dropdown in the second row with the text 'Select HTTP'. Below the table is a yellow warning box with an orange triangle icon and the text 'Warning: Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' To the right of the warning box is a green arrow pointing to the 'Review and Launch' button with the text 'Click "Review and Launch"'. At the bottom right are three buttons: 'Cancel', 'Previous', and 'Review and Launch' (highlighted in blue). At the bottom left is a copyright notice: '© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved.' and links for 'Privacy Policy' and 'Terms of Use'. At the bottom right is a 'Feedback' button.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

### Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

**Assign a security group:** ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Protocol	Type	Port Range (Code)	Source
SSH	TCP	22	Anywhere 0.0.0.0/0
HTTP	TCP	80	Anywhere 0.0.0.0/0

**Warning**

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Note: When the source IP of a rule is specified as “Anywhere” (0.0.0.0/0), a warning will appear that recommends using known IP addresses. The AMI will still work in this case, but you may wish to consult your network or IT security administrator to determine if it is necessary to use known IP addresses for your installation.

Click “Review and Launch” to continue.

The “Review Instance Launch” page provides a summary of the AMI details with a preview of all configuration settings that were made during the AMI instance creation process. Review the settings under each category and make any corrections by selecting the corresponding “Edit...” link. When finished, click the “Launch” button to start the AMI.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

### Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**⚠ Your instance configuration is not eligible for the free usage tier**


To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions.

[Don't show me this again](#)

**⚠ Improve your instance's security. Your security group, cypress\_group, is open to the world.**

Your instance may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

▼ AMI Details

 **Cypress v2.4.0 Public AMI - ami-8fb1fce6**  
Cypress v2.4.0 Public AMI  
Root Device Type: ebs Virtualization type: paravirtual

[Edit AMI](#)

▼ Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
m1.medium	2	1	3.7	1 x 410	-	Moderate

[Edit instance type](#)

▼ Security Groups

Security Group ID	Name	Description
sg-e74fb78c	cypress_group	Cypress Security Group

All selected security groups inbound rules

Security Group ID	Protocol ⓘ	Type ⓘ	Port Range (Code) ⓘ	Source ⓘ
sg-e74fb78c	SSH	TCP	22	0.0.0.0/0
sg-e74fb78c	HTTP	TCP	80	0.0.0.0/0

[Edit security groups](#)

[Cancel](#) [Previous](#) [Launch](#)

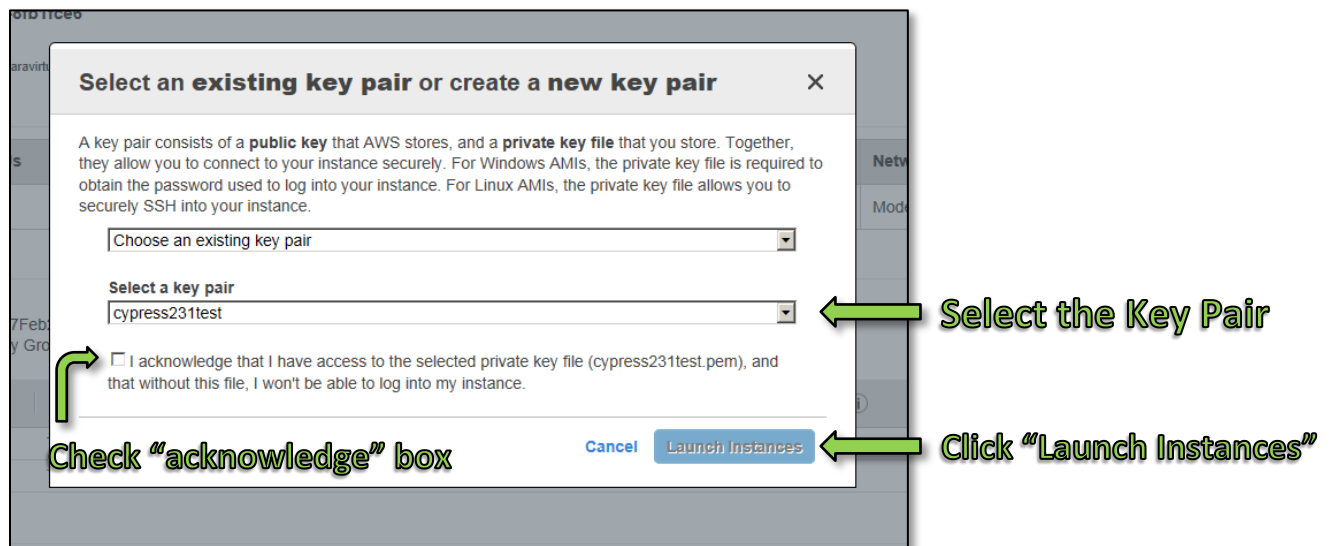
[Feedback](#)

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

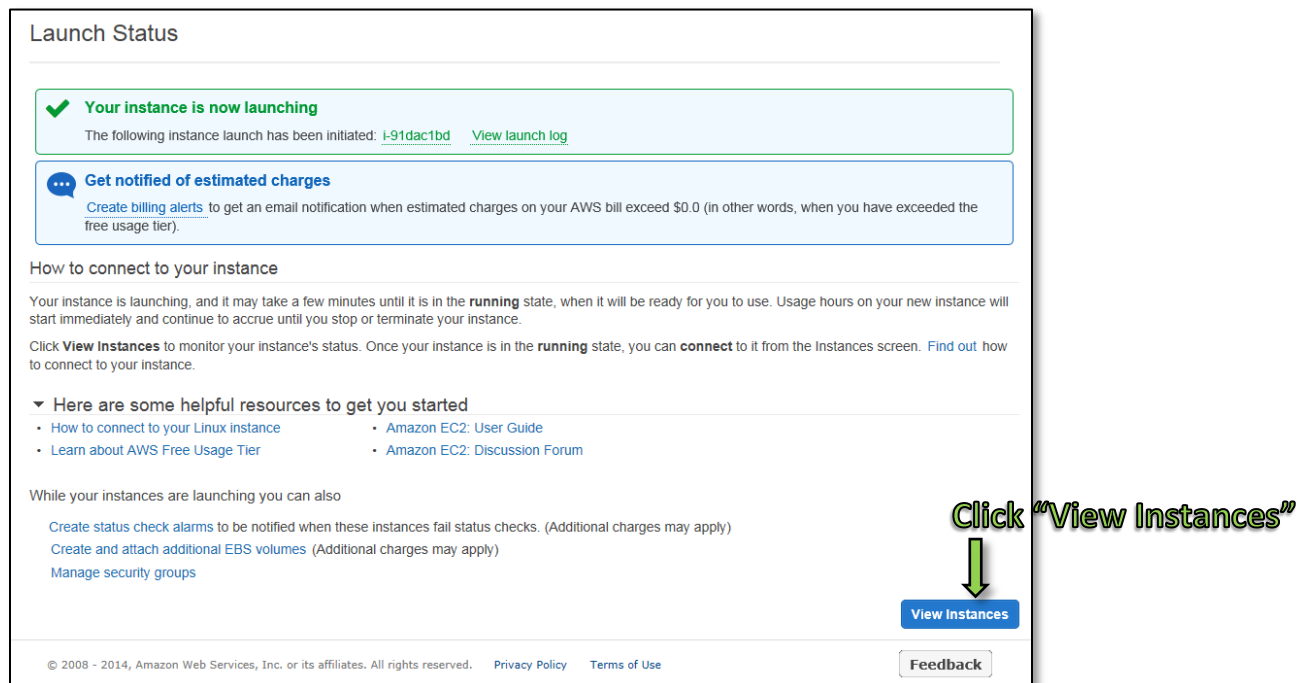
Click “Launch” to start the AMI



A dialog will appear for selecting the Key Pair (created earlier) to use with your AMI. Choose the correct Key Pair in the bottom pull down list, and confirm that you have the private key file for the selected Key Pair by checking the acknowledgement checkbox. If you do not have a Key Pair, you can still create one by selecting “Create a new key pair” in the top pull down list. The “Launch Instances” button will become enabled when the dialog has been properly completed.



The “Launch Status” screen will then appear indicating that the launch of your instance has been initiated. The initialization of newly launched instances can take a few minutes. Click the “View Instances” button to see the status of launched instances.

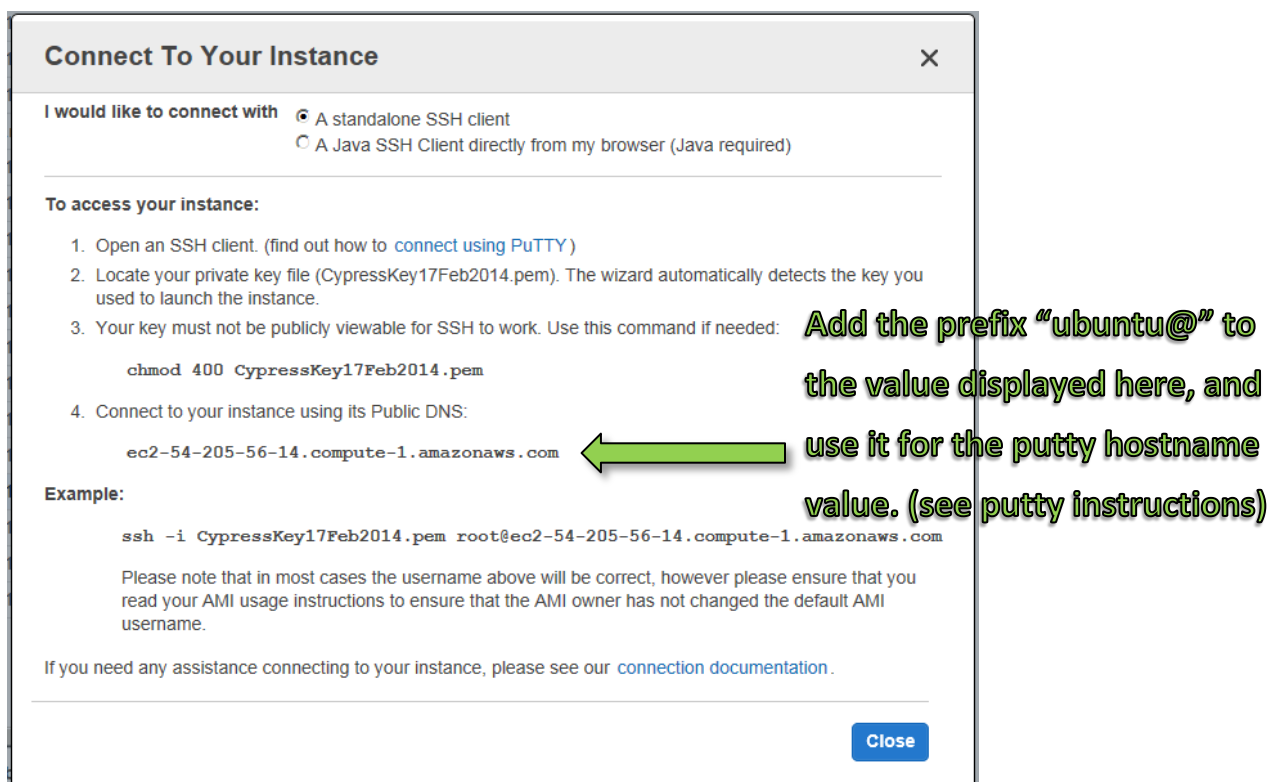
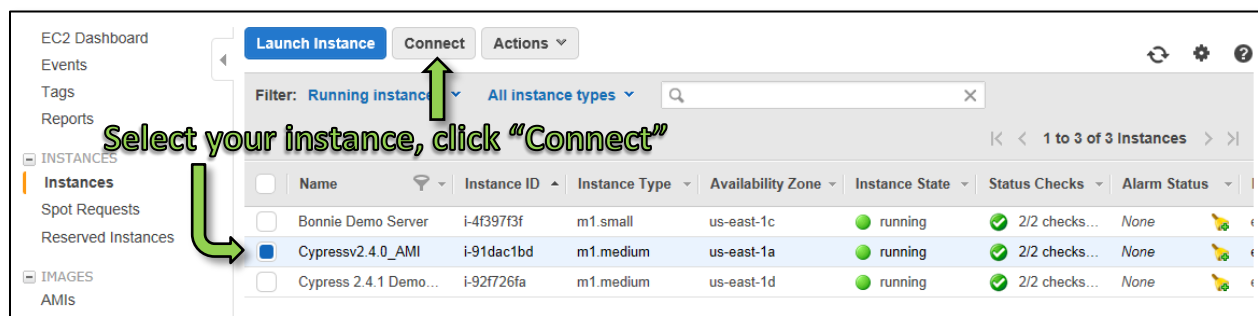


## Next Steps...

Some final configuration of the Cypress AMI is required before use. This involves updating the measures and value sets of your instance and upgrading your version of Cypress. In order to access measures and value set data, a National Library of Medicine (NLM) account is needed which can be requested here: <https://uts.nlm.nih.gov/license.html>.

Once your NLM account is ready, updating the measures and value sets is done via command line instructions on a SSH connection with the AMI. A popup window containing information on how to connect via SSH with your instance can be displayed by selecting your instance in the list of running instances, and clicking the "Connect" button.

Instructions for connecting from Windows with the putty SSH client are available at: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>



Once you have established a SSH connection with your AMI, follow these instructions to update the value sets and measures. Use the procedure that is specific to the version of Cypress you are installing. Regardless of which version is being installed, the value sets and the measures must be downloaded before using Cypress. This may take several minutes.

### **Cypress 2.0.0 or 2.0.1**

```
sudo ./install_cypress.sh --import --nlm_user <user> -- nlm_passwd <pass>
```

### **Cypress 2.1.0**

For Cypress 2.1.0 AMI installs please run the following commands once you log into the system, substituting your NLM username and password where relevant.

```
sudo su - cypress  
cd /home/cypress/cypress  
wget --user=username --password=password  
http://demo.projectcypress.org/bundles/bundle- latest.zip source  
/usr/local/rvm/scripts/rvm bundle exec rake bundle:import[./bundlelatest.  
zip,false,true] RAILS_ENV=production
```

### **Cypress 2.2., Cypress 2.3.\* and Cypress 2.4.\***

For Cypress 2.2.0, Cypress 2.3.\* and Cypress 2.4.\* AMI installations, please run the following commands once you log into the system. You will be prompted for your NLM Username and Password to download the value sets and measures.

```
sudo su - cypress  
cd /home/cypress/cypress  
bundle exec rake cypress:bundle_download_and_install RAILS_ENV=production
```

### **Cypress 2.4.0 Upgrade to v2.4.1**

For Cypress 2.4.0 users, the additional step of upgrading to Cypress v2.4.1 is recommended. These steps are performed over the same SSH connection established above. At some points in this process, the system may prompt you for the password for the machine instance connection. This is NOT the NLM password. If you connected using the hostname "ubuntu@<public-DNS-of-instance>" as directed above, the password is "CypressPwd".

```
sudo su - cypress  
cd /home/cypress/cypress  
rm -r tmp/cache/*  
git fetch origin  
git checkout -b 2.4.1 v2.4.1
```

```
bundle install  
bundle update health-data-standards  
sudo service apache2 restart  
sudo stop delayed_worker  
sudo start delayed_worker
```

-----

Once the bundle installation is complete, you can open up the Cypress application in a web browser. The hostname is the same hostname you used to connect with SSH, but without the username prefix “ubuntu@”. The URL will be similar to the following.

<http://ec2---xx---xxx---xxx---xxx.compute---1.amazonaws.com/>

Alternatively, you can use the public IP address for your instance in the URL instead of the hostname. This is displayed in the instances table accessed from the EC2 dashboard.

Once the Cypress application login screen comes up select the “Create new account” link, create a new account, and then log in.